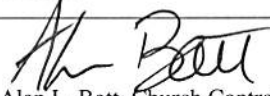


Financial Standard

Subject Accessing and Securing Financial Information		Number 6230
Prior Revision Date n/a	Current Revision Date June 3, 2013	 Alan L. Bott, Church Controller

1. PURPOSE

- 1.1. This financial standard emphasizes the critical need to control access to financial information and to safeguard this data at all times.

2. DEFINITIONS & ABBREVIATIONS

- 2.1. The [Financial Standards Glossary](#) can be accessed via this link.
- 2.2. Abbreviations:
CC = Church controller
LC = Local controller

3. STANDARDS

*Person/Group
Responsible*

- 3.1. The Church's financial statements, budgets, payroll, and other financial records are confidential or highly confidential. (See "Information and Systems Security Classification Policy" for classification details.) Management ensures that these records are accessed only by those who need them to perform their job duties and have been authorized to do so. *Management*
- 3.2. Data stewards determine the information classifications for confidentiality and privacy for all assigned data and information resources in accordance with Policy Point's "Information and Systems Security Classification Policy." Data stewards authorize access to information within their stewardship. Access to data is granted and terminated according to established procedures. *Data steward*
- 3.3. All finance personnel share responsibility for ensuring the confidentiality, integrity, and availability of financial information. Personnel understand and follow the Information and Communication policies in Policy Point that relate to accessing and securing financial information (see 4.1). *Finance personnel*
- 3.4. Employees must not divulge financial information outside of approved stewardships. Employees must be assured of a person's approved status to access financial information before sharing that information. Employees should be wary of social engineering and challenge suspicious or unfamiliar data requests. *Finance personnel*

- | | |
|--|--|
| 3.5. Management consults with the local controller and legal counsel to determine appropriate disclosures to any requesting legal or regulatory agency. The Church controller approves financial disclosures to any outside entity. | <i>Management,
LC, local legal
counsel, CC</i> |
| 3.6. Controllers perform periodic reviews of data access for people within their stewardship and modify access where appropriate. Finance managers and staff assist as assigned. | <i>Local
controller</i> |
| 3.7. Financial information in paper form and other non-digital media must be protected to the same degree as computerized information. Documents are shredded as appropriate. Employees safeguard information on desks, computer screens, white boards, etc. Employees avoid discussing confidential data where others may overhear. | <i>Finance
personnel</i> |
| 3.8. Electronic devices containing confidential or financial data must be physically secured at all times. Always lock laptops or other portable media in cabinets or desks overnight, even if office doors are locked. Never leave these devices in a car overnight or in unsafe locations while unattended. | <i>Finance
personnel</i> |
| 3.9. Highly confidential data should not be e-mailed and must be transmitted over external networks only with end-to-end encryption. Great care should be taken with confidential data as well—encryption is recommended. | <i>Finance
personnel</i> |
| 3.10. Highly confidential data must not be stored on portable media or devices (including laptops) except in rare cases authorized by the data steward. In these cases, the highly confidential data must be encrypted. The data must be securely overwritten (digitally shredded) as soon as possible. Great care should be taken with confidential data as well—encryption is recommended. | <i>Finance
personnel</i> |
| 3.11. Financial records are retained and destroyed in accordance with Financial Standard 6120 “Financial Records Management.” | <i>Finance
personnel</i> |
| 3.12. Employees must immediately report suspected breaches of information security to their supervisors and to the office of the chief information security officer via the Global Service Center. | <i>Finance
personnel</i> |
| 3.13. Failure to comply with this financial standard may subject an employee to disciplinary action, including termination of employment. | |

4. REFERENCES

- 4.1. Policy Point, Presiding Bishopric Departments, Policies, Information and Communication
- “Information Security Program & Policy”
 - “Data Stewardship Policy”
 - “Information and Systems Security Classification Policy”

4.2. Information and Communication Systems Department's IT Standards Library

- "Highly Confidential Data Handling Standard"
- "Mobile Device Security Standard"

4.3. Financial Standard 6120 "Financial Records Management"

4.4. https://dsp.ldschurch.org/Accord/domains/domain_list.jsf (list of data domains and data stewards)

5. EXHIBITS

5.1. Exhibit A: Access to Church Financial Data

Exhibit A:

ACCESS TO CHURCH FINANCIAL DATA

Financial Data	First Presidency	Quorum of the Twelve (a)	Presiding Bishopric	Presidency of the Seventy (a)	Seventy (a,g)	Area Presidency (a)	Finance and Records Managing Director/Church Controller/Financial Reporting (e)	Church Controller Representatives (f)	Treasury Services Authorized Employees (f)	Budget Office Authorized Employees (f)	ICS Employees Authorized by FRD (a)	Payroll Services Authorized Employees (f)	Global Service Center Authorized Employees (f)	Church Auditing (f)	HQ Department Executive Council/Managing Director/Controller (a)	DTA/Area Controller (a)	Local Unit Leader	Member
Tithing donations	Yes	Yes	Yes	Yes (h)	Yes (k)	Yes (h)	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes (n)	No
Fast offering donations	Yes	Yes	Yes	Yes (h)	Yes (k)	Yes (h)	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes (b)	Yes	Yes (n)	No
Fast offering expenditures	Yes	Yes	Yes	No	No	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes (b)	Yes (b)	Yes (n)	No
Other donations and revenue	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes (c)	Yes	Yes (n)	No
Operations expenditures	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes (c)	Yes	Yes (n)	No
Project expenditures	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes (c)	Yes	No	No
Program expenditures	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes (c)	Yes	No	No
Other expenditures	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes (c)	Yes	No	No
Cash	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	Yes	No	No
Investment securities	Yes	No	Yes	No	No	No	Yes	No	No	No	Yes	No	Yes	Yes	No	No	No	No
Investment properties	Yes	No	Yes	No	No	No	Yes	No	No	No	Yes	No	Yes	Yes	No	No	No	No
Other assets	Yes	No	Yes	No	No	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	No	Yes	No	No
Liabilities	Yes	No	Yes	No	No	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	No	Yes	No	No
Net assets	Yes	No	Yes	No	No	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	No	Yes	No	No
Personnel (salary, etc.)	Yes	No	Yes	No	No	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Financial records/amounts for an individual member (m)	Yes	Yes	Yes	Yes (h)	Yes (h)	Yes (h)	Yes	No	Yes	No	Yes	No	Yes	Yes	No	Yes (h)	Yes (n)	Yes (d)

(a) Only for departments/areas under their stewardship. Documentation of stewardship is retained by the function that provides confidential information to evidence the appropriateness of the access granted.

(b) Only Welfare Services Department has access to this information and formally documents which individuals are approved for access to different types of confidential information.

(c) Only has access to information for their own department/entity. Management's authorization of access to employees in their department is clearly justified based on the person's role and responsibilities and formally documented.

(d) Member's own information only or information of minor child living in home.

(e) Access for financial reporting employees is limited to their role and responsibilities and documented by the financial reporting manager.

(f) Each of these organizations determines information access needed for its employees based on the individual's role and responsibilities. These information access requests are submitted to, approved by, and documented by the Finance and Records Department's managing director and the Church controller.

(g) Area Seventy only have access to information through the Area Presidency.

(h) Only to be used in the process of selecting ecclesiastical leaders.

(k) May be shown over time only as ratio or index numbers.

(m) For more detailed guidelines, refer to MSR's "Member Leader Unit Information Release Policy" revised January 8, 2013.

(n) Only for his unit.

Note: Financial information is disclosed to outside entities only as required by law and approved by the Church controller.